Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (previously presented) A descrambler integrated circuit (IC) adapted to receive scrambled digital content, a message and an encrypted descrambling key, comprising:

a local memory to store a unique key;

a first process block to decrypt a message using the unique key to produce a key, the key being formed from a mating key generator being a message that comprises an identifier of a manufacturer of a digital device including the descrambler IC and an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider;

a second process block using the key to decrypt the encrypted descrambling key and to recover a descrambling key; and

a descrambler using the descrambling key to descramble the scrambled digital content and to produce digital content in a clear format.

2. (original) The descrambler IC of claim 1, wherein the unique key is loaded into the local memory during manufacture of the descrambler IC.

3. (original) The descrambler IC of claim 1, wherein the second process block is a finite state machine.

4. (previously presented) The descrambler IC of claim 1, wherein the key is formed by encrypting the mating key generator using the unique key.

5. (previously presented) The descrambler IC of claim 1, wherein the mating key generator further comprises an identifier that identifies a provider of a system that enables

transmission of the scrambled digital content and the mating key generator message to the descrambler IC.

6. (original) The descrambler IC of claim 5, wherein the mating key generator further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content and the mating key generator is transmitted, and (ii) a mating key sequence number.

7. (original) The descrambler IC of claim 1, wherein the first process block and the second process block are logic operating in accordance with one of the following: Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Triple DES.

8. (original) The descrambler IC of claim 1, wherein the unique key is a one-time programmable value that cannot be read or overwritten once programmed.

9-22. (canceled)

23. (previously presented) A descrambler integrated circuit (IC) adapted to receive scrambled digital content and to descramble the scrambled digital content, comprising:

a first process block to encrypt a message using a unique, one-time programmable key to produce a first key, the message includes a mating key generator being a message that comprises an identifier of at least one of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier;

a second process block to receive an encrypted second key and, using the first key, to decrypt the encrypted second key in order to recover the second key in a non-encrypted format, the encrypted second key; and

a descrambler using the second key in the non-encrypted format to descramble the scrambled digital content and to produce digital content in a clear format.

24. (original) The descrambler IC of claim 23, wherein the encrypted second key is an encrypted service key associated with at least one selected tier of service.

25. (original) The descrambler IC of claim 23, wherein the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC.

26. (canceled).

27. (previously presented) The descrambler IC of claim 23, wherein the mating key generator encrypted by the first process block using the unique key to produce a result being the first key.

28-31. (canceled)

32. (previously presented) A descrambler integrated circuit (IC) adapted to receive scrambled digital content, a message and an encrypted descrambling key, comprising:

a local memory to store a unique key;

a first process block controlled by a non-CPU based state machine to decrypt a message using the unique key to produce a key, the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier;

a second process block controlled by a non-CPU state machine using the key to decrypt the encrypted descrambling key and to recover a descrambling key; and

a descrambler using the descrambling key to descramble the scrambled digital content and to produce digital content in a clear format.

33. (previously presented) The descrambler IC of claim 32, wherein the unique key is loaded into the local memory during manufacture of the descrambler IC and cannot be read or overwritten once programmed.

34. (previously presented) The descrambler IC of claim 32, wherein the first process block and the second process block are logic operating in accordance with one of the following: Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Triple DES.

35. (previously presented) The descrambler IC of claim 23, wherein the encrypted second key is the second key encrypted to a mating key being a value retrieved from a remote server using the mating key generator and a serial number of a digital device implemented with the descrambler IC.